

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-134413

(43) 公開日 平成9年(1997)5月20日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 K 17/00			G 0 6 K 17/00	F E
G 0 9 C 1/00	6 1 0	7259-5 J	G 0 9 C 1/00	6 1 0 D
	6 3 0	7259-5 J		6 3 0 C
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 C
審査請求 未請求 請求項の数 3 O L (全 14 頁) 最終頁に続く				

(21) 出願番号 特願平7-289871

(22) 出願日 平成7年(1995)11月8日

(71) 出願人 000134257

株式会社トーキン

宮城県仙台市太白区郡山6丁目7番1号

(72) 発明者 三浦 融

宮城県仙台市太白区郡山六丁目7番1号

株式会社トーキン内

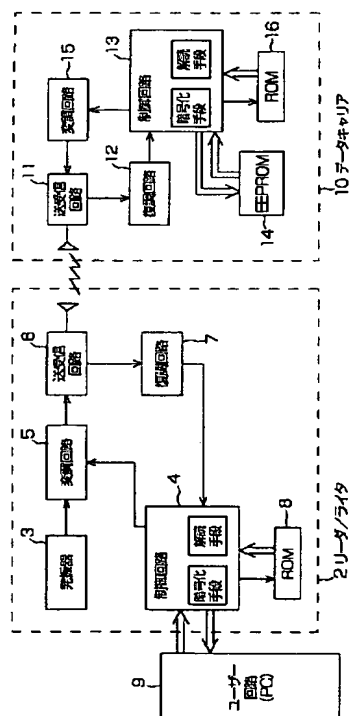
(74) 代理人 弁理士 後藤 洋介 (外3名)

(54) 【発明の名称】 非接触型データキャリアシステム

(57) 【要約】

【課題】 一連の通信毎に異なった暗号化処理を行なえる非接触型データキャリアシステムを提供すること。

【解決手段】 暗号化処理を決定づけるキーデータを複数用意しておき、リーダ/ライタ2内のROM8、及びデータキャリア10内のROM16又はEEPROM14に、該複数のキーデータからなるデータテーブルを記憶させておく。更に、通信開始時にリーダ/ライタ2及びデータキャリアの一方は、暗号化処理に用いるキーデータを決定し、該キーデータがデータテーブルの何処にあるのかを示す位置データを他方へ送信する。位置データを受信した該他方は、該位置データを用いてデータテーブルからキーデータを選択する。その後、一連の通信が終了するまで、リーダ/ライタ2及びデータキャリアの双方は、同じキーデータを用いた暗号化処理を行なう。



1 非接触型データキャリアシステム

【特許請求の範囲】

【請求項1】 無線にてデータ通信を互いに行うデータキャリアとリーダ／ライタとからなり、

該データキャリアは、書き込み可能なデータメモリを有し、読み取り指令に基づいて該データメモリ中のデータを読み出し、データキャリア側の送信信号として前記リーダ／ライタに送信する機能と、前記リーダ／ライタからの送信信号を受信信号として受信する機能と、該受信信号中の読み取り命令に応じて前記読み取り指令を送出する機能と、該受信信号中の書き込みデータを前記データメモリ中に書き込む機能とを有しており、

前記リーダ／ライタは、前記データキャリア側の送信信号を受信して前記データメモリ中のデータを取得する機能と、前記データメモリ中のデータを読み取るべき前記読み取り命令あるいは、前記データメモリ中に書き込むべき前記書き込みデータを前記リーダ／ライタ側の送信信号として送信する機能とを有してなる非接触型データキャリアシステムにおいて、

前記リーダ／ライタおよび前記データキャリアのそれぞれは、

両者間の通信データを暗号化処理するための複数の異なる暗号化キーデータをテーブルとして記憶するための暗号化キーデータメモリと、

通信開始時に該暗号化キーデータの中から特定の一つを特定暗号化キーデータとして選択し、送信データを該特定暗号化キーデータに基づき暗号化する暗号化手段と、受信信号を前記特定の暗号化キーデータに基づいて解読する解読手段とを有し、

これにより、一連の通信毎に、異なる暗号化処理を選択できることを特徴とする非接触型データキャリアシステム。

【請求項2】 請求項1の非接触型データキャリアシステムにおいて、

前記暗号化キーデータのテーブルは、各暗号化キーデータに固有のキーコードを有しており、

前記データキャリアは、前記リーダ／ライタ側送信信号を受信したときに、前記特定暗号化キーデータを選択する手段と、該特定暗号化キーデータのキーコードをキャリア側送信データの一つとして、前記リーダ／ライタに通知する手段とを有することを特徴とする非接触型データキャリアシステム。

【請求項3】 請求項1の非接触型データキャリアシステムにおいて、

前記暗号化キーデータのテーブルは、各暗号化キーデータに固有のキーコードを有しており、

前記リーダ／ライタは、その送信開始時に、前記特定暗号化キーデータを選択する手段と、該特定暗号化キーデータのキーコードをリーダ／ライタ側送信データの一つとして、前記リーダ／ライタに通知する手段とを有することを特徴とする非接触型データキャリアシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、読み出し及び書き換え可能なメモリと通信機能とを内蔵したICカード等からなりIDカード・定期券・プリペイドカード等に使用されるデータキャリアと、通信機能を有するリーダ／ライタとからなり、電磁結合方式、電磁誘導方式、光方式、電波方式等の非接触によるデータ通信によって、リーダ／ライタからデータキャリアに内蔵されたメモリへのデータの読みだし及び書き換えが可能である非接触型データキャリアシステムに関する。

【0002】

【従来の技術】現在、非接触型データキャリアシステムのデータキャリアとして一般的に使用されているものには、CPU・マスクROM・RAM・各種周辺素子等に電気的に書き換え可能なEEPROM (Electrically Erasable Programmable Read Only Memory) または書き換えのできないPROMを加えて構成した専用ICチップを内蔵したものと、ゲートアレイによりロジック回路を構成した専用ICにEEPROMまたはPROMを組み合わせて内蔵したもの等があり、塩化ビニル、樹脂モールド等により密封される。

【0003】これらのデータキャリアを有する非接触型データキャリアシステムは、外部とのデータ入出力用接続端子を有さず、電磁結合方式・電磁誘導方式・光方式・電波方式等により、非接触でリーダ／ライタとデータキャリア間のデータ通信を行い、リーダ／ライタからデータキャリア内のメモリに記憶されたデータの読みだし或いは書き換えを行えるようになっているため、水・塵・静電気等による影響がなく耐環境性に優れている。

【0004】また、これらの非接触型データキャリアシステムのデータキャリアは、接続端子又は磁気ヘッドに接触させる必要がある従来の接触型ICカード或いは磁気カードのように、リーダ／ライタへ挿入する手間もなく、専用のリーダ／ライタにかざすようにするだけで動作するため、操作性が向上している。

【0005】

【発明が解決しようとする課題】ここで、非接触型データキャリアシステムは、IDデータ・金銭データ等のデータを取り扱うため、当然のことながら、セキュリティが要求されることとなる。従って、非接触によるデータ通信には、そのデータ通信方式、データの変調／復調方式、データの構成など、様々な方法が採用されており、それらがセキュリティの向上に貢献している。

【0006】しかしながら、リーダ／ライタとデータキャリア間の双方の通信データの内容が解読困難であったとしても、通信信号自体、例えば電磁波や光などの変調信号を、通信を行っているリーダ／ライタ及びデータキャリア以外のコイルや受光素子等を用いて捕らえること

は容易である。このようにして、捕らえた信号と同一の信号をリーダ／ライタやデータキャリアに対して送信されると、誤動作をしてしまう可能性がある。また、このようなことが不正目的に利用されてしまうかもしれないことは、十分に予想されることである。

【0007】本発明は、このような問題点を解決すべくなされたもので、一連の通信開始時毎に、暗号化処理を決定づけるデータをキーデータとして、リーダ／ライタ又はデータキャリアのどちらかで決定する手段、リーダ／ライタ又はデータキャリアのどちらか一方で決定されたキーデータを、他方に通知する手段とを有し、一連の処理毎にキーデータを変更することで、常に暗号化処理が変化し、不正操作による誤動作を防止し、セキュリティを向上させる非接触データキャリアシステムを提供するものである。

【0008】

【課題を解決するための手段】即ち、本発明によれば、無線にてデータ通信を互いに行うデータキャリアとリーダ／ライタとからなり、該データキャリアは、書き込み可能なデータメモリを有し、読み取り指令に基づいて該データメモリ中のデータを読み出し、データキャリア側の送信信号として前記リーダ／ライタに送信する機能と、前記リーダ／ライタからの送信信号を受信信号として受信する機能と、該受信信号中の読み取り命令に応じて前記読み取り指令を送出する機能と、該受信信号中の書き込みデータを前記データメモリ中に書き込む機能とを有しており、前記リーダ／ライタは、前記データキャリア側の送信信号を受信して前記データメモリ中のデータを取得する機能と、前記データメモリ中のデータを読み取るべき前記読み取り命令あるいは、前記データメモリ中に書き込むべき前記書き込みデータを前記リーダ／ライタ側の送信信号として送信する機能とを有してなる非接触型データキャリアシステムにおいて、前記リーダ／ライタおよび前記データキャリアのそれぞれは、両者間の通信データを暗号化処理するための複数の異なる暗号化キーデータをテーブルとして記憶するための暗号化キーデータメモリと、通信開始時に該暗号化キーデータの中から特定のものを特定暗号化キーデータとして選択し、送信データを該特定暗号化キーデータに基づき暗号化する暗号化手段と、受信信号を前記特定の暗号化キーデータに基づいて解読する解読手段と、を有し、これにより、一連の通信毎に、異なる暗号化処理を選択できることを特徴とする非接触型データキャリアシステムが得られる。

【0009】また、本発明によれば、前記非接触型データキャリアシステムにおいて、前記暗号化キーデータのテーブルは、各暗号化キーデータに固有のキーコードを有しており、前記データキャリアは、前記リーダ／ライタ側送信信号を受信したときに、前記特定暗号化キーデータを選択する手段と、該特定暗号化キーデータのキーコードをキャリア側送信データの一つとして、前記リー

ダ／ライタに通知する手段とを有することを特徴とする非接触型データキャリアシステムが得られる。

【0010】更に、本発明によれば、前記非接触型データキャリアシステムにおいて、前記暗号化キーデータのテーブルは、各暗号化キーデータに固有のキーコードを有しており、前記リーダ／ライタは、その送信開始時に、前記特定暗号化キーデータを選択する手段と、該特定暗号化キーデータのキーコードをリーダ／ライタ側送信データの一つとして、前記リーダ／ライタに通知する手段とを有することを特徴とする非接触型データキャリアシステムが得られる。

【0011】

【発明の実施の形態】以下に、本発明の実施の形態を図面を用いて説明する。

【0012】本発明の実施の形態の非接触型データキャリアシステム1は、図1に示す様な、リーダ／ライタ2及びデータキャリア10から構成されている。

【0013】リーダ／ライタ2において、発振器3は、一定の周波数の信号を変調回路5へ送出し、また、CPUを中心に構成された制御回路4は、データキャリア10のEEPROM14に対するデータの読み出し或いは書き込みなどの要求を示すコマンドコード及びデータからなるコマンド電文を作成し、その作成したコマンド電文を変調回路5へ送出する。変調回路5は、発振器3より受けた信号を用いて、制御回路4から受けたコマンド電文を変調し、送受信回路6へ送出する。送受信回路6は、変調回路5から受けたコマンド電文をデータキャリア10へ送信する一方、データキャリア10から送信されてきた後述するレスポンス電文を受信し、その受信したレスポンス電文を復調回路7へ送出する。復調回路7は、送受信回路6から受けたレスポンス電文を復調し、制御回路4へ送出する。

【0014】一方、データキャリア10において、送受信回路11は、リーダ／ライタ2から送信されてきたコマンド電文を受信し、復調回路12へ送出する。復調回路12は、送受信回路11から受けたコマンド電文を復調し、制御回路13へ送出する。制御回路13は、復調回路12により復調されたコマンド電文に従い、EEPROM14に対して読み込み或いは書き込みを行なうと共に、レスポンスコード及びデータからなるレスポンス電文を作成し、その作成したレスポンス電文を変調回路15へ送出する。変調回路15は、制御回路13から受けたレスポンス電文を変調し、送受信回路11へ送出する。送受信回路11は、変調回路15から受けた変調されたレスポンス電文をリーダ／ライタ2へ送信する。

【0015】また、ユーザー回路9は、リーダ／ライタ2の制御を行なうものであり、本発明の実施の形態では、一例として、パーソナルコンピュータ(PC)を使用した。更に、リーダ／ライタ2内のROM8及びデータキャリア10内のROM16は、双方とも、それぞれ

の動作を制御するプログラムを記憶している。

【0016】ここで、本発明の実施の形態においては、リーダ／ライタ2内のROM8及びデータキャリア10内のROM16に、更に、暗号化処理のためのプログラム、及び暗号解読のためのプログラム、並びに、後述する様に、暗号化処理を決定づけるデータテーブルを記憶させてある。リーダ／ライタ2及びデータキャリア10は、これらのプログラムをそれぞれの制御回路が実行することにより、暗号化処理をソフト的に行なっている。

【0017】尚、上記のリーダ／ライタ2内のROM8及びデータキャリア10内のROM16に記憶されている暗号化処理のためのプログラムと、及び暗号解読のためのプログラムと、並びに暗号化処理を決定づけるデータテーブルと、それらのプログラムを実行している制御回路の機能を持つ様な回路又はそれらの内の一部の機能を実行する様な回路を別に構成し、暗号化処理をハード的に行なってもよい。

【0018】次に、本発明の実施の形態における暗号化処理について説明する。

【0019】まず、本発明の実施の形態の非接触型データキャリアシステム1において、リーダ／ライタ2とデータキャリア10との間の通信で使用される暗号化処理のアルゴリズムは、予め、決定されている。ここで、簡単な例として、 $y = (x \text{ XOR } a) + b$ という関数を用いて暗号化処理を説明する。尚、 y は暗号化処理した結果の1バイトデータを、 x は暗号化処理する前の1バイトデータを、 a 及び b はこの暗号化処理を決定づける各1バイトのキーデータを示すものである。暗号化処理は、この式を用いて、単純な排他的論理和(XOR)と加算によって行なわれている。尚、この計算は、1バイト毎に行なわれ、桁上げが生じた場合には無視するものとする。暗号解読処理は、暗号化処理に用いた式を逆に計算して行なえばよく、 $x = (y - b) \text{ XOR } a$ となる。

【0020】これらの暗号化処理を決定づけるのは、 a 及び b といったキーデータである。本発明の非接触型データキャリアシステム1においては、これらのキーデータを複数組み用意し、リーダライタ2内のROM8、及びデータキャリア10内のROM16或いはEEPROM14に、図2に示す様な、同一のデータテーブルとして記憶させてある。ここで、図2において、 n とあるのは、各キーデータのコード、即ちキーコードであり、この実施の形態においては、どのキーデータがデータテーブルの何番目にあるのかを示す位置データである。

【0021】データキャリア10がリーダ／ライタ2との通信領域に入り、通信によりお互いの存在が確認された時に、リーダ／ライタ2及びデータキャリア10のいずれかにおいて、前述の a 及び b といったキーデータを無作為に選択決定する。更に、リーダ／ライタ2及びデータキャリア10の一方は、キーデータを選択決定する

と、その選択決定されたキーデータのデータテーブルにおける位置を示す位置データを、通信により他方に通知する。

【0022】リーダ／ライタ2及びデータキャリア10の一方が、他方にどのキーデータを選択決定したのかを示す位置データを他方に通知すると、双方ともが同一のキーデータを認識することができるため、これ以後の通信は、選択決定されたキーデータ、即ち a 及び b を用いて、リーダ／ライタ2とデータキャリア10との間で送受信されるデータの内容に対し、それぞれ暗号化処理及び暗号解読処理を行ない、暗号化処理されたデータによって行なわれることになる。尚、ここで、キーデータは、一連の通信が終了するまで同一のものをを用いることとする。

【0023】これにより、通信自体が暗号化されるため、解読が困難になることに加え、一連の通信毎に暗号化を決定づけるキーデータが変わるため、不正目的により以前に捕らえられた通信信号を真似た信号が外部から送出されてきたとしても、次の一連の通信では内容を正しく解読することができないため、誤動作を防げることになる。また、暗号化処理を決定づける選択決定されたキーデータは、通信上に直接現れることがないため、暗号化処理されたデータの解読を更に困難なものとしている。

【0024】以上に説明してきたことは、以下に示す第1及び第2の実施の形態について共通のことである。

【0025】(第1の実施の形態) 以下に、第1の実施の形態の非接触型データキャリアシステム1の動作を図3乃至図6を用いて説明する。

【0026】第1の実施の形態の非接触型データキャリアシステム1は、データキャリア10が暗号化を決定づけるキーデータを選択決定し、その選択決定されたキーデータのデータテーブルにおける位置を示す位置データをリーダ／ライタ2に通知することにより暗号化処理を行なったデータの通信を可能とするものである。

【0027】まず、図3を用いてリーダ／ライタ2の動作を説明する。リーダ／ライタ2は、図5に示されるコマンド電文フォーマットに従って、起動コマンドをコマンドコードにセットし、一定の周期で起動コマンドを含むコマンド電文を送信している(S101)。ここで、図5中のSTX(02)は、コマンド電文開始コードを、ETX(03)は、コマンド電文の終了コードを意味し、BCC(Block Check Character)は、STXの次からETXまでの排他的論理和(XOR)の計算結果をセットすることを意味する。次に、リーダ／ライタ2は、データキャリア10が通信可能な領域にあれば、データキャリア10がこのコマンド電文に対するレスポンス電文を送信してくるため、このレスポンス電文の受信の有無を判定する(S102)。リーダ／ライタ2は、データキャリア10からのレスポンス電文を受信しない

10

20

30

40

50

限り、ステップS101へ戻り、コマンド電文を送信し続ける。データキャリア10からのレスポンス電文を受信すると、そのレスポンス電文には、後述する様に、データキャリア10の選択決定したキーデータのデータテーブルにおける位置を示す位置データが含まれているため、リーダ/ライタ2は位置データを取得する(S103)ことができる。リーダ/ライタ2は、位置データを取得すると、それに基づいて、複数のキーデータからなるデータテーブルから、データキャリア10の選択決定したキーデータを選択する(S104)。

【0028】リーダ/ライタ2は、これ以降、一連の通信が終了するまで、このキーデータを用いて暗号化処理された電文にてデータキャリア10との通信を行なう。

【0029】リーダ/ライタ2は、ステップS104において選択されたキーデータを用いて、コマンド電文フォーマットに従ったコマンド電文のコマンドコードとデータに、暗号化手段により、暗号化処理を施して暗号化されたコマンド電文を作成し、データキャリア10に暗号化されたコマンド電文を送信する(S105)。データキャリア10がこのコマンド電文を受信すると、このコマンド電文に対する暗号化されたレスポンス電文を送信してくるため、リーダ/ライタ2は、このレスポンス電文の受信の有無を判定する(S106)。リーダ/ライタ2は、データキャリア10からのレスポンス電文を受信しない限り、ステップS105へ戻り、暗号化されたコマンド電文をデータキャリア10に送信し続ける。リーダ/ライタ2は、暗号化されたレスポンス電文を受信すると、暗号解読手段により、暗号化されたレスポンス電文を解読する(S107)。その後、通信を終了するかどうかを判定し(S108)、通信を終了しない場合は、ステップS105に戻り、更に一連の動作を繰り返す。通信を終了する場合、リーダ/ライタ2は、通信終了を意味するコマンドコードを含むコマンド電文に対し、暗号化手段により、暗号化処理を施して暗号化されたコマンド電文を作成し、データキャリア10に暗号化された通信終了を意味するコマンド電文を送信する(S109)。データキャリア10がこのコマンド電文を受信すると、このコマンド電文に対する暗号化されたレスポンス電文を送信してくるため、リーダ/ライタ2は、このレスポンス電文の受信の有無を判定する(S110)。リーダ/ライタ2は、データキャリア10からのレスポンス電文を受信しない限り、ステップS109へ戻り、暗号化されたコマンド電文をデータキャリア10に送信し続ける。リーダ/ライタ2は、暗号化されたレスポンス電文を受信すると、暗号解読手段により、暗号化されたレスポンス電文を解読し(S111)、一連の通信を終了する。

【0030】次に、図4を用いて、データキャリア10の動作について説明する。データキャリア10は、電源(図示せず)から供給を受けると、位置データの値nに

初期値として0をセットする(S201)。その後、リーダ/ライタ2からの起動コマンドを含むコマンド電文を受信するまで、一定の周期で起動コマンドを含むコマンド電文を受信したかどうかの判定を行なう(S202)。データキャリア10は、このコマンド電文を受信しない限り、位置データの値nに1を加え(S203)、ステップS202へ戻る。ここで、本実施の形態において用いられるデータテーブルは、図2に示されているものであるため、位置データに上限がある。したがって、ステップS203において、1を加えた後、更に、nの値が0Fhを越えた場合、nの値から10hを引くこととしている。次に、データキャリア10は、リーダ/ライタ2からの起動コマンドを含むコマンド電文を受信すると、nの値から、位置データの決定を行ない(S204)、その決定した位置データに従い、データテーブルからキーデータを選択決定する(S205)。その後、データキャリア10は、図6のレスポンス電文フォーマットに従い、レスポンスコードと位置データの値をセットしたレスポンス電文を作成し、作成したレスポンス電文をリーダ/ライタ2へ送信する(S206)。ここで、図6に示されるレスポンス電文中のSTX(02)、ETX(03)、BCCは、前述したコマンド電文におけるものと同じ意味を持つものである。

【0031】データキャリア10は、これ以降、一連の通信が終了するまで、このキーデータを用いて暗号化処理された電文にてリーダ/ライタ2との通信を行なう。

【0032】ここで、図2のデータテーブルを用いて、暗号化処理についての説明をする。暗号化処理は、前述したコマンド電文においてはコマンドコードとデータに対して、レスポンス電文においては、レスポンスコードとデータに対して行なわれる。例えば、データキャリア10が決定した位置データが8であったとすると、aとbからなるキーデータは、それぞれa=71h、b=F2hとなる。また、コマンドコード又はレスポンスコードが31、データが55であったとすると、暗号化処理を施される前のコマンド電文又はレスポンス電文は、02 31 55 03 67 となる。このコマンド電文又はレスポンス電文の、コマンドコード或いはレスポンスコード、及びデータに対して、 $y = (x \oplus 71) + F2$ の暗号化処理が行なわれると、02 32 16 03 27 となる。逆に、暗号解読処理は、 $x = (y - F2) \oplus 71$ の式にて行なわれる。

【0033】データキャリア10は、リーダ/ライタ2から、暗号化処理されたコマンド電文を受信すると(S207)、暗号化処理されたコマンド電文に対し、選択決定したキーデータを用いて暗号解読処理を行ない、暗号化処理されたコマンド電文を解読する(S208)。次に、データキャリア10は、暗号解読されたコマンド電文が通信終了を指示するものかどうかを判定する(S209)。コマンド電文が通信終了を指示するものでな

い場合、データキャリア10は、暗号化処理したレスポンス電文をリーダ/ライタ2へ送信し（S210）、ステップS207へ戻り、次の暗号化処理されたコマンド電文を受信するまで待機をする。ステップS209において、暗号解読されたコマンド電文が通信終了を指示するものであった場合、データキャリア10は、そのコマンド電文に対応する暗号化処理されたレスポンス電文を作成し、リーダ/ライタ2へ送信し（S211）、一連の通信を終了する。

【0034】このようにして、本発明の第1の実施の形態におけるデータキャリア10及びリーダ/ライタ2からなる非接触型データキャリアシステム1は、一連の通信毎に、暗号化処理に用いるキーデータを変えることができ、各通信毎に異なる暗号化処理を行なうことが可能となった。

【0035】（第2の実施の形態）次に、第2の実施の形態の非接触型データキャリアシステム1の動作を図5乃至図8を用いて説明する。

【0036】第2の実施の形態の非接触型データキャリアシステム1は、第1の実施の形態とは異なり、リーダ/ライタ2が暗号化を決定づけるキーデータを選択決定し、その選択決定されたキーデータのデータテーブルにおける位置を示す位置データをデータキャリア10に通知することにより暗号化処理を行なったデータの通信を可能とするものである。また、暗号化処理及び暗号解読処理は、第1の実施の形態と同じものとした。

【0037】まず、図7を用いてリーダ/ライタ2の動作を説明する。リーダ/ライタ2は、位置データの値nに初期値0をセットする（S301）。次に、リーダ/ライタ2は、図5に示されるコマンド電文フォーマットに従って、起動コマンドをコマンドコードにセットし、一定の周期で起動コマンドを含むコマンド電文を送信する（S302）。次に、リーダ/ライタ2は、データキャリア10が通信可能な領域にあれば、データキャリア10がこのコマンド電文に対するレスポンス電文を送信してくるため、このレスポンス電文の受信の有無を判定する（S303）。リーダ/ライタ2は、データキャリア10からのレスポンス電文を受信しなかった場合、位置データの値nに1を加え（S304）、ステップS202へ戻り、コマンド電文を送信し続ける。ここで、nが0Fを越えた場合は、第1の実施の形態のデータキャリア10のステップS203における動作と同じ動作を行なう。

【0038】データキャリア10からのレスポンス電文を受信すると、リーダ/ライタ2は、nの値から位置データを決定し（S305）、その位置データに従い、データテーブルから暗号化処理に用いるキーデータを決定する（S305）。その後、リーダ/ライタ2は、位置データを含むコマンド電文をデータキャリア10に送信し（S307）、データキャリア10からのレスポンス

電文を受信したかどうかを判定する（S308）。ステップS308において、データキャリア10からのレスポンス電文が受信されなかった場合、リーダ/ライタ2は、ステップS307に戻り、再び位置データを含むコマンド電文をデータキャリア10に送信する。

【0039】一方、ステップS308において、データキャリア10からのレスポンス電文を受信した場合、リーダ/ライタ2は、これ以降、一連の通信が終了するまで、選択決定したキーデータを用いて暗号化処理された電文にてデータキャリア10との通信を行なう。

【0040】ステップS308において、データキャリア10からのレスポンス電文を受信すると、リーダ/ライタ2は、選択決定したキーデータを用いて、コマンド電文フォーマットに従ったコマンド電文のコマンドコードとデータに、暗号化手段により、暗号化処理を施して暗号化されたコマンド電文を作成し、データキャリア10に暗号化されたコマンド電文を送信する（S309）。データキャリア10がこのコマンド電文を受信すると、このコマンド電文に対する暗号化されたレスポンス電文を送信してくるため、リーダ/ライタ2は、このレスポンス電文の受信の有無を判定する（S310）。リーダ/ライタ2は、データキャリア10からのレスポンス電文を受信しない限り、ステップS309へ戻り、暗号化されたコマンド電文をデータキャリア10に送信し続ける。リーダ/ライタ2は、暗号化されたレスポンス電文を受信すると、暗号解読手段により、暗号化されたレスポンス電文を解読する（S311）。その後、通信を終了するかどうかを判定し（S312）、通信を終了しない場合は、ステップS309に戻り、更に一連の動作を繰り返す。通信を終了する場合、リーダ/ライタ2は、通信終了を意味するコマンドコードを含むコマンド電文に対し、暗号化手段により、暗号化処理を施して暗号化されたコマンド電文を作成し、データキャリア10に暗号化された通信終了を意味するコマンド電文を送信する（S313）。データキャリア10がこのコマンド電文を受信すると、このコマンド電文に対する暗号化されたレスポンス電文を送信してくるため、リーダ/ライタ2は、このレスポンス電文の受信の有無を判定する（S314）。リーダ/ライタ2は、データキャリア10からのレスポンス電文を受信しない限り、ステップS313へ戻り、暗号化されたコマンド電文をデータキャリア10に送信し続ける。リーダ/ライタ2は、暗号化されたレスポンス電文を受信すると、暗号解読手段により、暗号化されたレスポンス電文を解読し（S315）、一連の通信を終了する。

【0041】次に、図8を用いて、データキャリア10の動作について説明する。データキャリア10は、電源（図示せず）から供給を受けると、その後、リーダ/ライタ2からの起動コマンドを含むコマンド電文を受信するまで、一定の周期で起動コマンドを含むコマンド電文

を受信したかどうかの判定を行なう（S401）。データキャリア10は、リーダ／ライタ2からの起動コマンドを含むコマンド電文を受信すると、図6のレスポンス電文フォーマットに従いレスポンス電文を作成し、作成したレスポンス電文をリーダ／ライタ2へ送信する（S402）。次に、リーダ／ライタ2が送信してくる位置データを含むコマンド電文を受信すると（S403）、データキャリア10は、このコマンド電文に対するレスポンス電文を作成し、そのレスポンス電文をリーダ／ライタ2へ送信する（S404）。送信後、前述の受信したコマンド電文に含まれる位置データを用いて、データテーブルから、リーダ／ライタ2の選択決定したキーデータを選択する（S405）。

【0042】データキャリア10は、これ以降、一連の通信が終了するまで、このキーデータを用いて暗号化処理された電文にてリーダ／ライタ2との通信を行なう。

【0043】データキャリア10は、リーダ／ライタ2から、暗号化処理されたコマンド電文を受信すると（S406）、暗号化処理されたコマンド電文に対し、選択決定したキーデータを用いて暗号解読処理を行ない、暗号化処理されたコマンド電文を解読する（S407）。次に、データキャリア10は、暗号解読されたコマンド電文が通信終了を指示するものかどうかを判定する（S408）。コマンド電文が通信終了を指示するものでない場合、データキャリア10は、暗号化処理したレスポンス電文をリーダ／ライタ2へ送信し（S409）、ステップS406へ戻り、次の暗号化処理されたコマンド電文を受信するまで待機をする。ステップS408において、暗号解読されたコマンド電文が通信終了を指示するものであった場合、データキャリア10は、そのコマンド電文に対応する暗号化処理されたレスポンス電文を作成し、リーダ／ライタ2へ送信し（S410）、一連の通信を終了する。

【0044】このようにして、本発明の第2の実施の形態におけるデータキャリア10及びリーダ／ライタ2からなる非接触型データキャリアシステム1は、一連の通信毎に、暗号化処理に用いるキーデータを変えることができ、各通信毎に異なる暗号化処理を行なうことが可能となった。

【0045】尚、本実施の形態においては、暗号化処理の動作を簡単に説明するために、一例として、前記の簡単な式、及び図2に示す様な内容のデータテーブルを用いてきたが、式及びデータテーブルの内容は、任意に選択及び決定することができ、本実施の形態に制限されない。

【0046】また、本実施の形態において、位置データnの決定方法は、単純に1を加算して、特定条件が満たされるまでループさせるものであったが、乱数を発生させて行なう方法などでもよく、本実施の形態に制限されない。

【0047】また、決定した位置データを内部メモリに記憶させ、次回通信を行なう時に同一データとならない様にもすることも可能である。

【0048】また、本実施の形態において、暗号化処理及び暗号解読処理は、コマンド電文のコマンドコード及びデータ、及びレスポンス電文のレスポンスコード及びデータに対して行なってきたが、コマンドコード及びレスポンスコード、又はデータのどちらか一方だけに処理を行なってもよく、本実施の形態に制限されない。

10 【0049】また、本実施の形態において、コマンド電文及びレスポンス電文は、それぞれ図5及び図6に示されるものを用いたが、他のフォーマットを用いてもよく、本実施の形態に制限されない。

【0050】更に、本実施の形態において、上記の式及びデータテーブルを用いた暗号化処理は、各通信毎に一度しか行なっていないが、例えば、データテーブルにmとして、各通信毎に何回暗号化処理を行なうかを示すデータを予め記憶させておき、それに従い、暗号化処理を行なってもよい。

20 【0051】

【実施例】実施の形態において、通信の方式は、電磁結合方式を採用した。

【0052】

【発明の効果】以上説明した様に、本発明によれば、非接触型データキャリアシステムにおけるデータキャリアとリーダ／ライタとの間の通信に用いられる暗号化処理を決定づけるキーデータを、直接通信上に現すことなく指定でき、更に、一連の通信毎にキーデータを変更することにより、各通信毎に異なった暗号化処理を行なえ、通信のセキュリティが向上した非接触型データキャリアシステムを提供することができる。

【図面の簡単な説明】

【図1】本発明の非接触型データキャリアシステムを示すブロック図である。

【図2】本発明の実施の形態において用いたデータテーブルを示す図である。

【図3】本発明の第1の実施の形態におけるリーダ／ライタの動作概略を示す流れ図である。

30 【図4】本発明の第1の実施の形態におけるデータキャリアの動作概略を示す流れ図である。

【図5】本発明の実施の形態において用いたコマンド電文を示す図である。

【図6】本発明の実施の形態において用いたレスポンス電文を示す図である。

【図7】本発明の第2の実施の形態におけるリーダ／ライタの動作概略を示す流れ図である。

【図8】本発明の第2の実施の形態におけるデータキャリアの動作概略を示す流れ図である。

【符号の説明】

50 1 非接触型データキャリアシステム

- 2 リーダ／ライタ
- 3 発振器
- 4 制御回路
- 5 変調回路
- 6 送受信回路
- 7 復調回路
- 8 ROM
- 9 ユーザー回路 (PC)

【図2】

n	a	b
0	15	34
1	F4	8B
2	2A	E5
3	36	AA
4	B3	4C
5	AC	03
6	60	C2
7	9E	44
8	71	F2
9	D0	D6
A	81	15
B	F2	9C
C	24	89
D	BB	27
E	C2	B1
F	05	8F

データテーブル

【図5】

STX (02)	コマンドコード	データ	ETX (03)	BOC
-------------	---------	-----	-------------	-----

リーダ／ライタ コマンド電文フォーマット

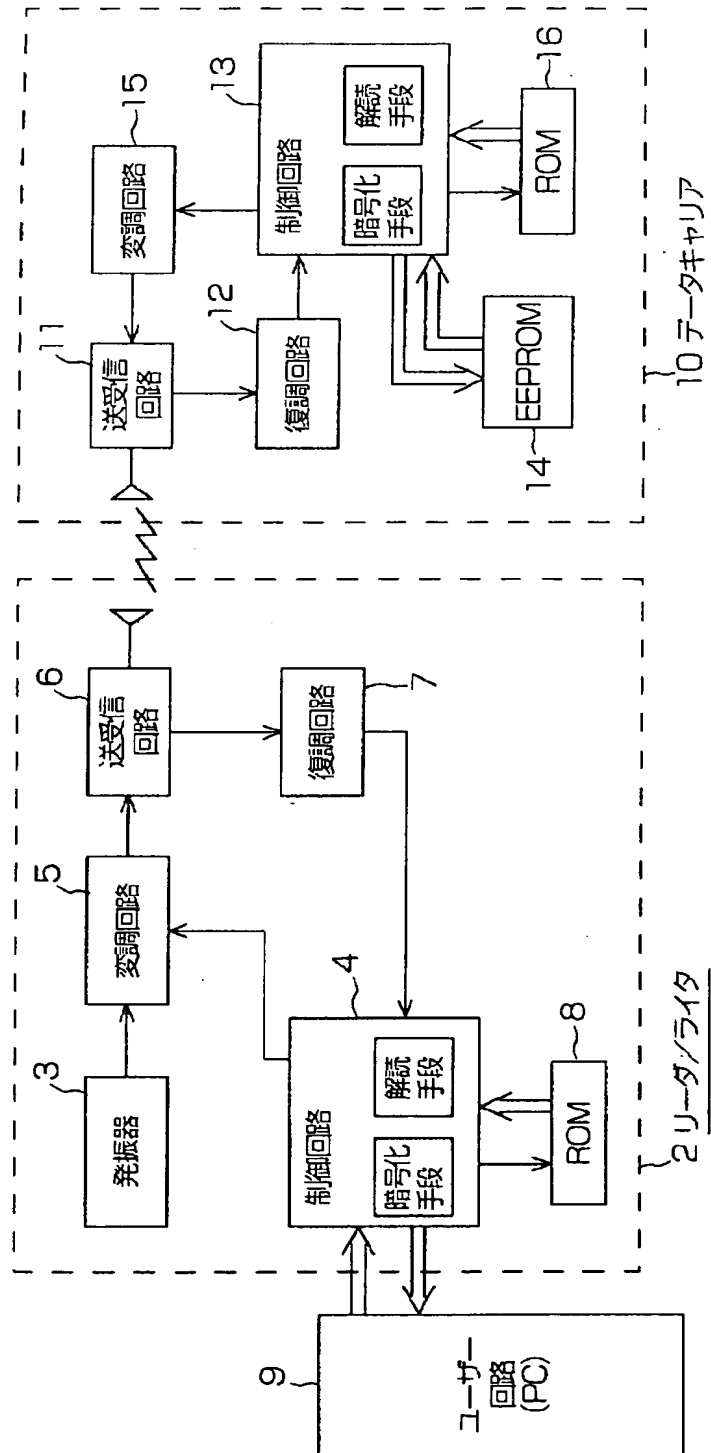
- 10 データキャリア
- 11 送受信回路
- 12 復調回路
- 13 制御回路
- 14 EEPROM
- 15 変調回路
- 16 ROM

【図6】

STX (02)	レスポンスコード	データ	ETX (03)	BOC
-------------	----------	-----	-------------	-----

データキャリア レスポンス電文フォーマット

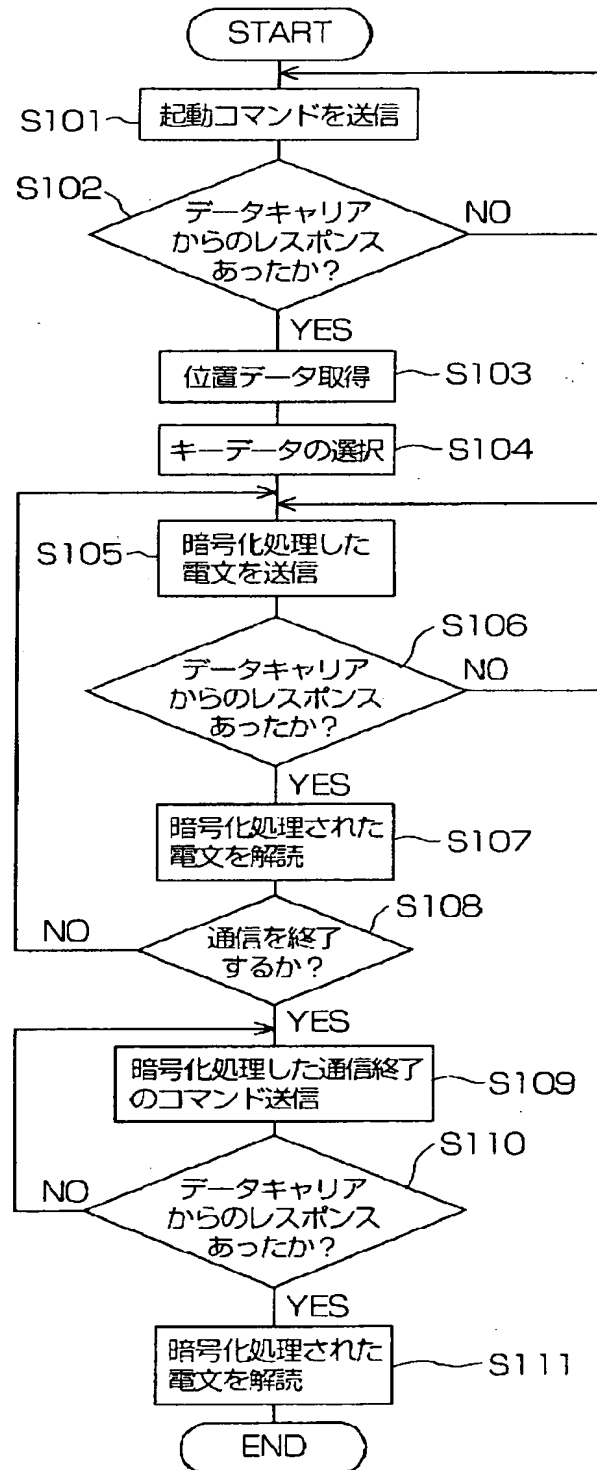
【図1】



1 非接触型データキャリアシステム

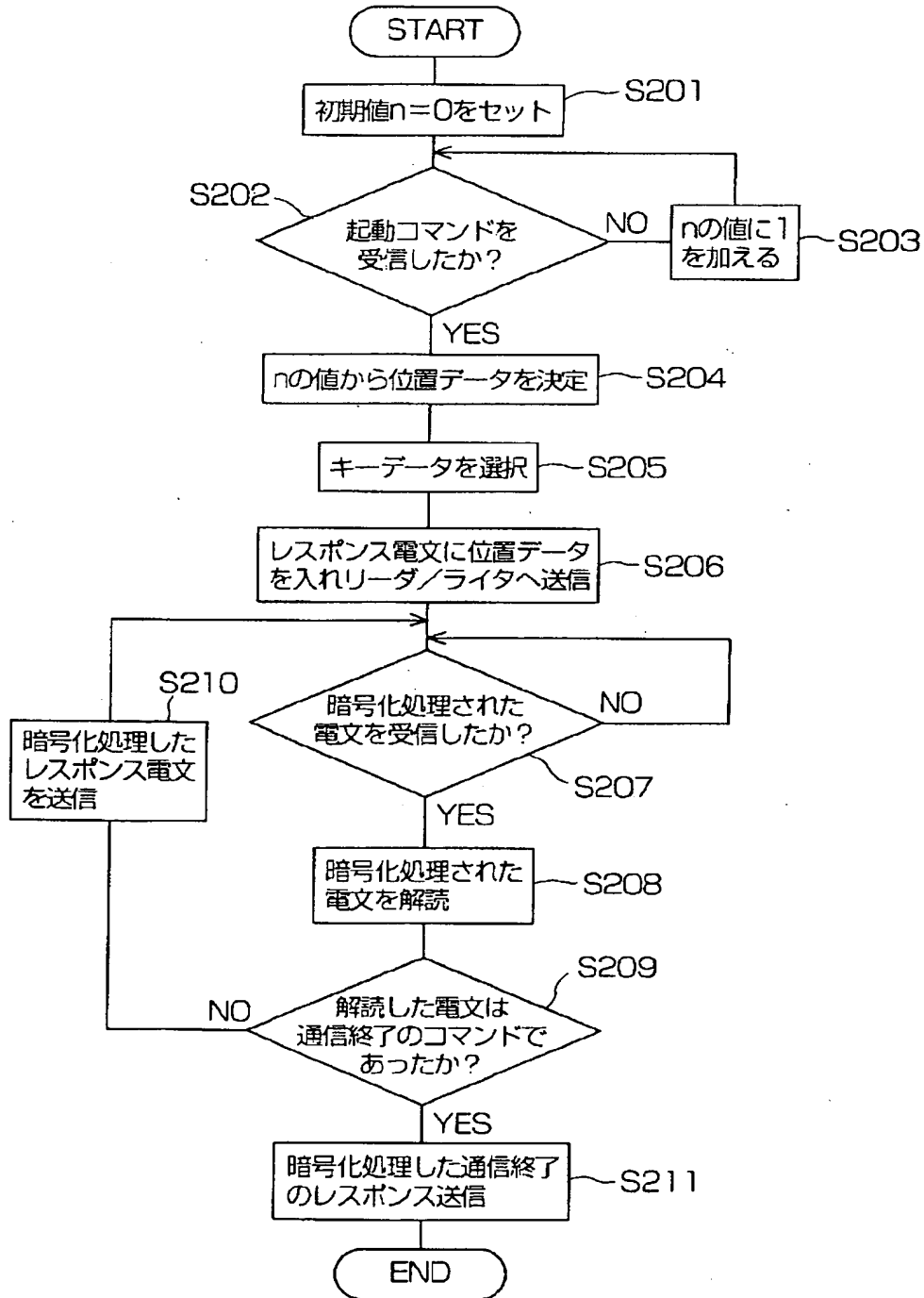
【図3】

データキャリアが位置データを決定する場合の
リーダー/ライタの動作概略フローチャート



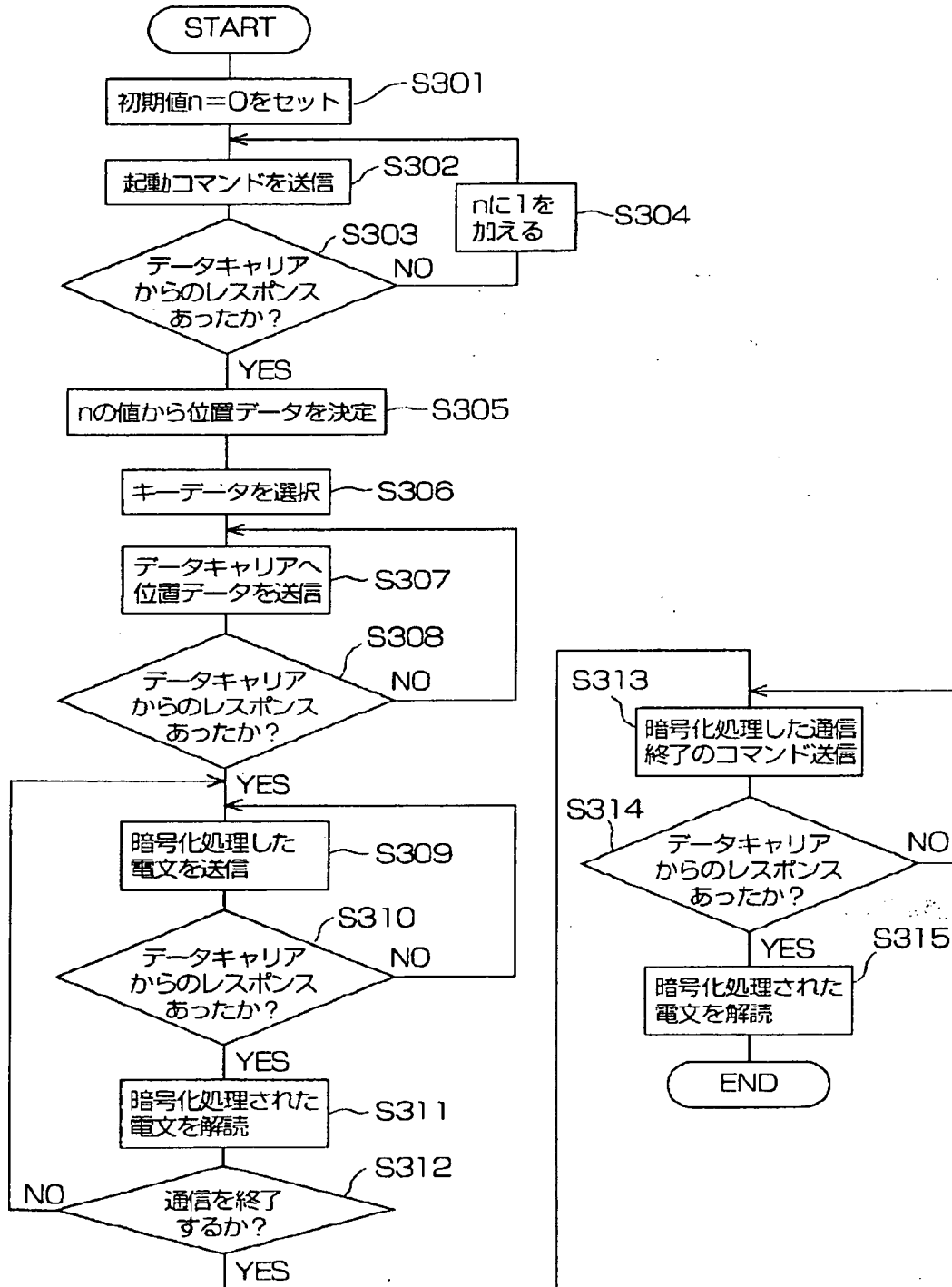
【図4】

データキャリアが位置データを決定する場合の
データキャリアの動作概略フローチャート



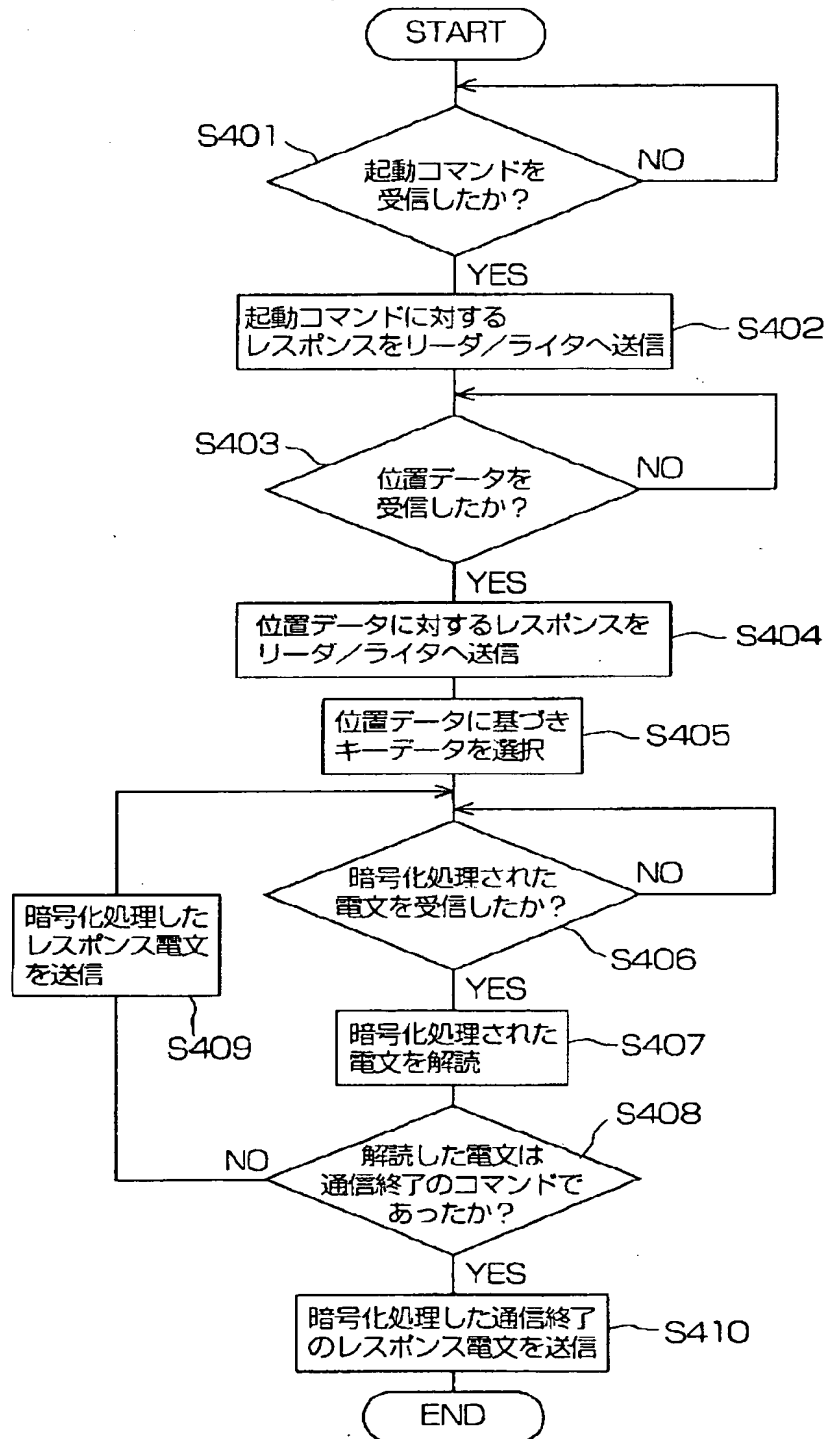
【図7】

リーダー/ライターが位置データを決定する場合の
リーダー/ライターの動作概略フローチャート



【図8】

リーダ/ライタが位置データを決定する場合の
データキャリアの動作概略フローチャート



フロントページの続き

(51)Int. Cl.⁶H 0 4 L 9/18
12/28

識別記号

庁内整理番号

F I

H 0 4 L 9/00
11/00

技術表示箇所

6 5 1
3 1 0 B